What is claimed:

1. A method of improving security processing in a computing network, comprising steps of:

providing a security offload component which performs security processing;

providing control functions in an operating system kernel for directing operation of the security offload component;

providing an application program;

executing the application program; and

executing the provided control functions during execution of the application program, thereby selectably directing the security offload component to secure at least one communication of the executing application program.

2. The method according to Claim 1, wherein the executing control functions include a function directing the security offload component to begin securing the communications.

3. The method according to Claim 1, wherein the executing control functions include a function directing the security offload component to stop securing the communications.

4. The method according to Claim 2, wherein the function further specifies information to be used by the security offload component.

5. The method according to Claim 4, wherein the specified information comprises one or more of: authentication information; cipher suites options; and security key input information.

6. The method according to Claim 1, wherein the control functions further inform protocol layers of the operating system kernel to modify outbound data in preparation for use by the security offload component.

7. The method according to Claim 6, wherein the modifications include reserving space in the outbound data for security headers and trailers.

8. The method according to Claim 1, wherein the control functions include providing client and/or server certificates to the security offload component for use in securing the communications.

9. The method according to Claim 1, wherein the control functions include providing one or more keys or key rings to the security offload component for use in securing the communications.

10. The method according to Claim 1, wherein the control functions include providing an identification of a encryption algorithm to the security offload component for use in securing the communications.

11. The method according to Claim 1, wherein secured outbound data of the executing application is thereby sent to its destination directly from the security offload component, after a single pass over a data bus from a protocol stack of the operating system kernel.

12. A system for improving security processing in a computing network, comprising:

a security offload component which performs security processing;

at least one control function in an operating system kernel for directing operation of the security offload component;

means for executing the at least one provided control function; and

means, responsive to operation of the means for executing, for directing the security offload component to secure at least one communication of an application program.

13. A computer program product for improving security processing in a computing network, the computer program product embodied on one or more computer-readable media and comprising:

a security offload component which performs security processing;

at least one control function in an operating system kernel for directing operation of the security offload component;

computer-readable program code means for executing the at least one provided control function; and

computer-readable program code means, responsive to operation of the computer-readable program code means for executing, for directing the security offload component to secure at least one communication of an application program.